

DEVICE FOR ENCRYPTING BINARY INFORMATION

Publication number: RU2007884 (C1)

Publication date: 1994-02-15

Inventor(s): BEREZIN BORIS V [RU] +

Applicant(s): BEREZIN BORIS V [RU] +

Classification:

- international: *H04L9/00; H04L9/00; (IPC1-7): H04L9/00*

- European:

Application number: SU19915012759 19911122

Priority number(s): SU19915012759 19911122

Abstract not available for **RU 2007884 (C1)**

Data supplied from the *espacenet* database — Worldwide



(19) RU⁽¹¹⁾ 2 007 884⁽¹³⁾ C1
(51) МПК⁵ H 04 L 9/00

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 5012759/09, 22.11.1991

(46) Дата публикации: 15.02.1994

(71) Заявитель:

Березин Борис Владимирович

(72) Изобретатель: Березин Борис Владимирович

(73) Патентообладатель:

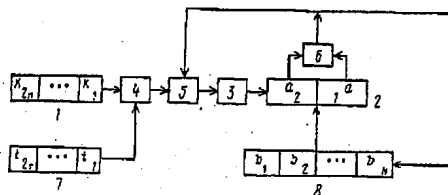
Березин Борис Владимирович

(54) УСТРОЙСТВО ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ "АЛБЕР"

(57) Реферат:

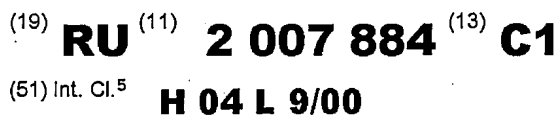
Использование: в технике криптографических преобразований в связанных, вычислительных и информационных системах для криптографического закрытия двоичной информации. Сущность изобретения: устройство содержит n-байтный ключевой регистр 1, однобайтный информационный регистр 2, блок 3 функционального преобразования, первый, второй, третий четырехразрядные сумматоры 4 - 6 по модулю два, g-байтный регистр 7, N-битный регистр 8. Обеспечивается возможность реализации устройства на микросхеме, содержащей всего лишь 2 тыс. вентилей, использования ключа такой длины,

которая обеспечивает невозможность его опробования за разумное время. Устройство улучшает криптографические и эксплуатационные параметры устройства шифрования. 2 з. п. ф-лы, 1 ил.



RU 2 007 884 C1

RU 2 007 884 C1



Изобретение относится к криптографическим преобразованиям и может быть использовано в связанных, вычислительных и информационных системах для криптографического закрытия двоичной информации.

Цель изобретения - упрощение аппаратной реализации устройства шифрования до возможности его размещения на микросхеме, содержащей не более 2 тысяч вентилях, а также использование ключа такой длины, которая обеспечивает невозможность его опробования за разумное время.

На чертеже представлена блок-схема предлагаемого устройства.

Устройство шифрования двоичной информации содержит 8-разрядный ключевой регистр 1, 8-разрядный информационный регистр 2, блок 3 четырехразрядный функционального преобразования f , первый, второй, третий четырехразрядные сумматоры 4-6 по модулю два, 8г-разрядный регистр 7 и N -разрядный регистр 8.

Устройство шифрования двоичной информации работает следующим образом.

Выработка полубайта шифрограммы $Ш$ осуществляется следующим образом.

1. В 8-разрядный информационный регистр 2 из N -разрядного регистра 8 записываются восемь бит, например, младших, b_{j1}, \dots, b_{j8} (или два полубайта, $a_2(i), a_1(i)$) исходной информации. Здесь b_1, \dots, b_N - содержимое N -разрядного регистра 8, $b_j = 0, 1, j = 1, N$.

2. Устройство работает пять циклов, все циклы работы идентичны. В i -й, $1 \leq i \leq s$ цикл работы к сумме i -го (по модулю $2n$) полубайта ключевого регистра 1 и i -го (по модулю $2r$) полубайта ключевого регистра 7 прибавляется сумма первого и второго полубайтов 8-разрядного информационного регистра 2, полученная схема преобразуется блоком 3 и результат записывается в 8-разрядный информационный регистр 2 на освободившееся место после сдвига его содержимого на один полубайт в сторону младших разрядов (вправо). После i -го цикла содержимое 8-разрядного информационного регистра 2 следующее:

$$a_2(i+1) = f(k_i \text{ (mod } 2n) +$$

$$+ t_i \text{ (mod } 2r) + (a_1(i) + a_2(i)),$$

$a_1(i+1) = a_2(i), i = > 1$, где $a_2(i), a_1(i)$ - два полубайта 8-разрядного информационного регистра 2 перед началом i -го цикла, $1 \leq i \leq s$;

$a_2(i), a_1(i)$ - исходное состояние регистра 2;

$a_2(s+1), a_1(s+1)$ - результирующее состояние регистра 2,

k_1, \dots, k_{2n} - $2n$ полубайт - n -байтного ключа,

t_1, \dots, t_{2r} - $2r$ полубайт содержимого регистра 2;

$+$ - сложение полубайтов по модулю 2 либо 2^4 ,

f - функция 2^4 -значной логики (система 4-двоичных функций от 4-двоичных переменных);

$a_1(i), a_2(i), k_i, t_i \in \{0, 1, \dots, 15\}, i = > 1$.

Если выбрать третий четырехразрядный сумматор 6 по модулю 2^4 , а первый и второй четырехразрядные сумматоры 4 и 5 по модулю 2, к ключевому полубайту прибавлять сначала полубайт из регистра 7, а затем уже

сумму полубайтов регистра 2, то после i -го цикла содержимое 8-разрядного информационного регистра 2 следующее:

$$a_2(i+1) = f(k_i \text{ (mod } 2n) \oplus t_i \text{ (mod } 2r) \oplus (a_1(i) \oplus a_2(i)),$$

$$a_1(i+1) = a_2(i), i = > 1$$

\oplus - поразрядное сложение полубайтов по модулю 2;

\oplus - сложение полубайтов по модулю 2^4 .

3. Сумма полученных в 8-разрядном информационном регистре 2 после s -го цикла двух полубайт $a_1(s+1), a_2(s+1)$ является полубайтом шифрограммы $Ш$, т. е. $Ш = a_1(s+1) \oplus a_2(s+1)$.

В блоке 3 реализуется функция 2^4 -значной логики, представленная в дизъюнктивной форме системой четырех двоичных функций y_1, \dots, y_4 от четырех двоичных переменных $x_1, \dots, x_4, y_1, x = 0, 1, i = 1, 4$.

В качестве функционального преобразования f можно выбрать, например, следующее:

$$y_1 = x_1x_4 \vee x_1x_2x_4 \vee x_1x_2x_3x_4 \vee x_1x_2x_3x_4$$

$$y_2 = x_2x_3 \vee x_2x_3x_4 \vee x_1x_2x_3x_4 \vee x_1x_2x_3x_4$$

$$y_3 = x_1x_2x_3 \vee x_1x_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4$$

$$y_4 = x_2x_3x_4 \vee x_1x_2x_3 \vee x_1x_2x_3 \vee x_2x_3x_4$$

Увеличение числа циклов работы устройства шифрования повышает уверенность в криптографической надежности зашифрования информации, т. е. в том, что никому не удастся расшифровать сообщение за время, меньшее чем полное опробование всех возможных вариантов n -байтного ключа. Вместе с тем, чем больше циклов работает устройство для выработки одного полубайта шифрограммы, тем меньше его производительность. Это дает возможность выбора между риском и производительностью. Рекомендуется выбирать число 5 циклов работы устройства шифрования в пределах от $4n$ до $16n$, где n - длина ключа в байтах. Реальная длина ключа - от 8 до 16 байт.

Для выработки следующего полубайта шифрограммы используются 8 бит b_{j1}, \dots, b_{j8} следующего состояния N -разрядного регистра 8.

В качестве N -разрядного регистра 8 можно выбрать 15-разрядный регистр сдвига со следующей линейной функцией максимального периода $2^{15} - 1$ в обратной связи: $b_{16} = b_1 \oplus b_2$. Если текущее состояние регистра сдвига обозначить через b_1, \dots, b_{15} , где $b_i = 0, 1, i = 1, 15$, то следующее состояние регистра сдвига будет $b_2, \dots, b_{15}, b_1 \oplus b_2$.

В 8г-разрядный регистр 7 записывается представленное в двоичном виде текущее время (месяц, число, час, минута, секунда) или случайное число, выработанное датчиком случайных чисел. Вместе с временем или случайным числом можно записывать также и номер передающего абонента. Реальная длина регистра 87 - 4-8 байт. Очередное состояние 8г-разрядного регистра 7 используется для выработки 2^{N-1} полубайт шифрограммы $Ш$, после чего в 8г-разрядный регистр 7 записывается новое время или новое случайное число.

При использовании единого времени оно не должно повторяться все время действия ключа. Например, если ключ действует один год, то время должно включать в себя месяц, если ключ действует несколько лет, то также и год.

После установки нового состояния в 8г-разрядный регистр 7 устройство шифрования формирует новое начальное состояние N-разрядного регистра 8. В случае 15-разрядного битного двоичного регистра сдвига можно предложить следующую процедуру формирования нового начального состояния.

Устройство шифрования прокручивается 5 циклов, как это было описано. Полученные после m-го, 3m-го, 5m-го, 7m-го циклов, где m это целая часть числа $8^{-1} s$, 4 полубайта

$$a_2(m+1) + a_1(m+1),$$

$$a_2(3m+1) + a_1(3m+1),$$

$$a_2(5m+1) + a_1(5m+1),$$

$a_2(7m+1) + a_1(7m+1)$ записываются в регистр 8. В старшие два бита полубайта $a_2(7m+1) + a_1(7m+1)$ принудительно записываются знаки 1. Так как в выбранном регистре 8 всего 15 разрядов, то четвертый бит последнего полубайта не используется.

Очередное состояние 8г-разрядного регистра 7 и новое исходное состояние 15-разрядного двоичного регистра 8 сдвига используются для выработки 2¹⁴-полубайт (-2¹⁶ бит) шифрграммы, после чего требуется обновление состояния регистров 7 и 8.

Шифрграмма Ш складывается по модулю 2 с представленным в двоичном виде открытым сообщением А. Полученное зашифрованное сообщение В = А ⊕ Ш вместе с заполнением 8г-разрядного регистра 7 передается получателю.

Принимающий абонент устанавливает в 8г-разрядный регистр 7 своего устройства шифрования принятые г байт и вырабатывает описанным способом шифрграмму Ш. Затем принимающий абонент складывает ее по модулю 2 с принятым зашифрованным сообщением В и получает открытое сообщение А = В ⊕ Ш. (56) Сяо Д., Керр Д.

и Мэдник С. Защита ЭВМ. М.: Мир, 1982, с. 137-162.

Формула изобретения:

1. Устройство шифрования двоичной информации, содержащее ключевой регистр и последовательно соединенные блок многоразрядного функционального преобразования f и информационный регистр, отличающееся тем, что в нем ключевой регистр выполнен в виде n-разрядного ключевого регистра, информационный регистр выполнен в виде 8-разрядного информационного регистра, блок многоразрядного функционального преобразования f выполнен в виде блока 4-разрядного функционального преобразования, при этом в него введены первый, второй и третий 4-разрядных сумматора и г-разрядный регистр, причем выход ключевого регистра подключен к первому входу первого сумматора, выход которого подключен к первому входу второго сумматора, выход второго сумматора подключен к входу блока 4-разрядного функционального преобразования f, выход которого подключен к второму четырехразрядному входу информационного регистра, оба четырехразрядных выхода которого подключены к двум входам третьего сумматора, выход третьего сумматора подключен к второму входу первого сумматора, если г-разрядный регистр подключен к второму входу второго сумматора, или к второму входу второго сумматора, если г-разрядный регистр подключен к второму входу первого сумматора.

2. Устройство по п. 1, отличающееся тем, что в него дополнительно введен N-разрядный регистр, причем 8-разрядный выход N-разрядного регистра подключен к входу 8-разрядного информационного регистра.

3. Устройство по п. 1, отличающееся тем, что вход N-разрядного регистра подключен к выходу третьего четырехразрядного сумматора.

45

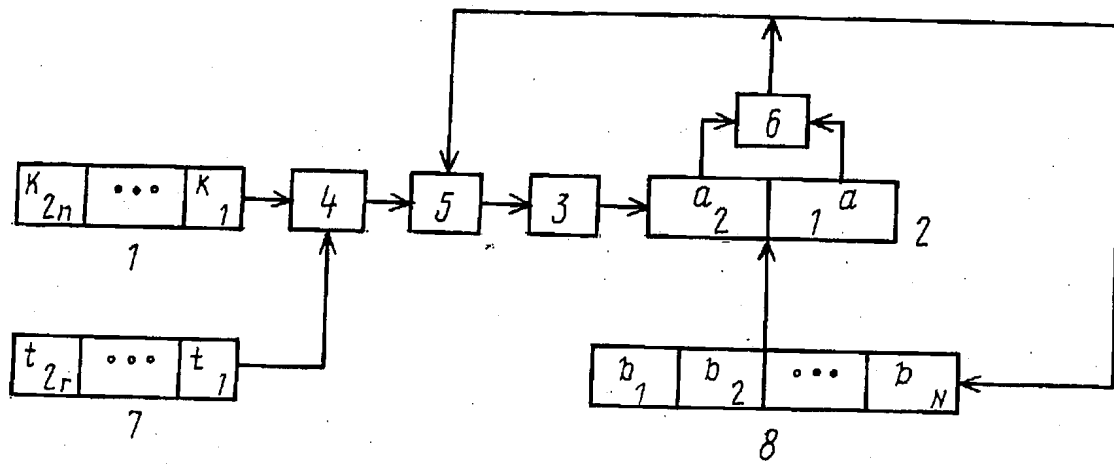
50

55

60

-4-

RU 2007884 C1



RU 2007884 C1